REMARKS

The foregoing amendment and the following remarks are submitted in response to the Office Action mailed on March 8, 2005 in connection with the above-identified application.

Claims 1-35 are pending in the present application. Claims 23-35 have been withdrawn as not being directed to an elected invention. Claims 1-22 have not been amended. Applicant respectfully submits that no new matter has been added to the application by the Amendment.

In a telephone conference between the undersigned and the Examiner in charge of the above-identified matter on or about March 4, 2005, the Examiner set forth a restriction requirement by identifying two groups: I - with claims 1-22 and II - with claims 23-35. After due consideration, the undersigned orally elected group I for further prosecution in connection with the present application. Applicant hereby affirms such election of group I without prejudice to the filing of a continuation application to further prosecute the invention of group II. Consistent with such election, Applicant has withdrawn un-elected claims 23-35.

The Examiner has rejected claims 1, 3-6, 8-9, 11, 13, and 14 under 35 USC § 102(b) as being anticipated by Saito (U.S. Patent No. 6,002,772). Applicant respectfully traverses this Section 102(b) rejection.

Independent claim 1 as originally presented recites a method for rendering encrypted digital content on a first device that has a public key (PU1) and a corresponding private key (PR1), where the digital content is encrypted according to a content key (KD). In the method, a digital license corresponding to the content is obtained, presumably by a second device or the like such as that recited in claims 5-7 on behalf of the first device, and

presumably from a license server or the like. The digital license includes the content key (KD) therein in an encrypted form.

Such second device or the like thus decrypts the encrypted content key (KD) from the digital license to produce the content key (KD), obtains from the first device the public key thereof (PU1), and encrypts the content key (KD) according to the public key (PU1) of the first device (PU1 (KD)). With such (PU1(KD)), then, the second device or the like composes a sub-license corresponding to and based on the obtained license. In particular, the sub-license includes (PU1 (KD)), and is transferred to the first device. Thus, the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key (KD).

As was set forth in detail in the present application, the invention as recited in claim 1 may be employed in the situation where the first device cannot itself directly communicate with the license server or the like to obtain the license. Instead, the second device or the like communicates with the license server on behalf of the first device to obtain the license. However, such license server provides the license with the content key (KD) therein encrypted in a manner accessible only by the second device, such as for example by being encrypted according to a public key of the second device. Thus, the license cannot be directly employed by the first device. Accordingly, the second device constructs a sub-license for the first device, where the sub-license is based on the license and has the content key (KD) therein encrypted according to the public key of the first device (PU1) to result in (PU1(KD)). Thus, and again, the first device can decrypt (PU1 (KD)) with the private key

thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key (KD).

The Saito reference discloses a method by which encrypted content may be distributed to and employed by a first user, and also by which the user may re-distribute the content to a second user. In the method, and referring generally to the first embodiment as shown in Fig.1, the first user requests the content by identifying same to a data center, along with a public key and other information. In response, and in pertinent part, the data center provides first and second content keys encrypted according to the public key of the first user, and the content encrypted according to the first content key. Thus, the first user applies a corresponding private key thereof to the encrypted first and second content keys to reveal same, and then applies the first content key to the encrypted content to reveal same, after which the first content key may be discarded. The first user then applies the second content key to the decrypted content to again encrypt same, and stores the encrypted content for later retrieval and use.

At a later time when the first user decides to re-distribute the encrypted content to a second user, the first user does not also distribute the decrypting second key with such encrypted content. Instead, the second user identifies the content to the data center, along with a public key and other information. In response, and in pertinent part, the data center provides the second content key and a third content key encrypted according to the public key of the second user, with the presumption that the content as possessed by the second user is already encrypted according to the second content key. Thus, the second user applies a corresponding private key thereof to the encrypted second and third content keys to reveal same, and then applies the second content key to the encrypted content to reveal same,

after which the second content key may be discarded. The second user then applies the third

content key to the decrypted content to again encrypt same, and stores the encrypted content

for later retrieval and use.

Notably, the Saito reference is entirely silent with regard to any license or sub-

license being employed to convey the encrypted content keys, as is required by claim 1. At

any rate, neither the first Saito user nor any other actor in the Saito reference obtains a

content key (KD) in an encrypted form, decrypts the encrypted content key (KD) to produce

the content key (KD), and encrypts the content key (KD) according to the public key (PU1)

of a first device (PU1 (KD)), as is required by claim 1. At most, each Saito user decrypts an

encrypted content key, but by no means does such Saito user encrypt the decrypted content

key according to the public key (PU1) of any other user or device. Instead, the Saito

reference teaches that only the data center performs any encryption of a content key

according to a public key.

Moreover, no Saito user composes any sub-license corresponding to and based

on any obtained license to include (PU1(KD)), as is required by claim 1. Again, only the

Saito data center is disclosed as encrypting any content keys, and not any Saito user.

Accordingly, Applicant respectfully submits that the Saito reference cannot be

applied to anticipate claim 1 or any claims depending therefrom, including claims 3-6, 8-9,

11, 13, and 14. Thus, Applicant respectfully requests reconsideration and withdrawal of the

Section 102(b) rejection.

The Examiner has also rejected 2, 7, 10, 12, and 15-22 under 35 USC § 103 as

being obvious over the Saito reference. Applicant respectfully traverses the Section 103

rejection.

Applicants respectfully submit that since independent claim 1 has been shown to be unanticipated and is non-obvious, then so too must all claims depending therefrom be unanticipated and non-obvious, including claims 2, 7, 10, and 12, at least by their dependencies.

With regard to independent claim 15, Applicant respectfully submits that such claim 15 recites essentially the same subject matter as claim 1, although from the point of view of the first device. In particular, after providing the public key (PU1) to the second device, and receiving the composed sub-license from the second device, the first device obtains (PU1 (KD)) from the received sub-license, applies (PR1) to (PU1 (KD)) to obtain the content key (KD), applies (KD) to decrypt the encrypted content, and renders the decrypted content.

Again, Applicant respectfully points our that the Saito reference is entirely silent with regard to any license or sub-license being employed to convey the encrypted content keys, as is required by claim 15. At any rate, neither the first Saito user nor any other actor in the Saito reference obtains a content key (KD) in an encrypted form from a sub-license based on a license to another user or device, as is required by claim 15. In particular, no Saito user or other actor sub-licenses to another use or other actor based on a received license, where the license and sub-license each include a content key (KD) encrypted in a form decryptable by the recipient of such license or sub-license, as is required by claim 15. Instead, in the Saito reference, only the data center performs any encryption of a content key, and not any Saito user.

Accordingly, Applicant respectfully submits that the Saito reference cannot be applied to make obvious claim 15 or any claims depending therefrom, including claims 16-
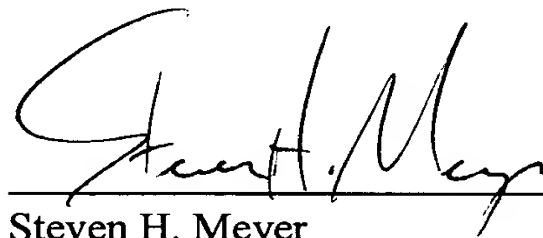
22. Thus, Applicant respectfully requests reconsideration and withdrawal of the Section 103 rejection.

In view of the foregoing, Applicants respectfully submit that the claims of the present application are in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

Date: May 18, 2005

Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439